

109TH CONGRESS
1ST SESSION

S. _____

To require financial services providers to maintain customer information security systems and to notify customers of unauthorized access to personal information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. CORZINE (for himself, _____) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To require financial services providers to maintain customer information security systems and to notify customers of unauthorized access to personal information, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Financial Privacy Pro-
5 tection Act of 2005”.

1 **SEC. 2. PREVENTION OF IDENTITY THEFT; NOTIFICATION**
2 **OF UNAUTHORIZED ACCESS TO CUSTOMER**
3 **INFORMATION.**

4 Subtitle B of title V of the Gramm-Leach-Bliley Act
5 (15 U.S.C. 6821 et seq.) is amended—

6 (1) by striking section 525;

7 (2) by redesignating sections 522 through 524
8 as sections 523 through 525, respectively;

9 (3) in section 525, as redesignated, by striking
10 “section 522” and inserting “section 523”; and

11 (4) by inserting after section 521 the following:

12 **“SEC. 522. PREVENTION OF IDENTITY THEFT; NOTIFICA-**
13 **TION OF UNAUTHORIZED ACCESS TO CUS-**
14 **TOMER INFORMATION.**

15 **“(a) CUSTOMER INFORMATION SECURITY SYSTEM**
16 **REQUIRED.—**

17 **“(1) IN GENERAL.—**In accordance with regula-
18 tions issued under paragraph (2), each financial in-
19 stitution shall develop and maintain a customer in-
20 formation security system, including policies, proce-
21 dures, and controls designed to prevent any breach
22 with respect to the customer information of the fi-
23 nancial institution.

24 **“(2) REGULATIONS.—**

25 **“(A) IN GENERAL.—**Each of the Federal
26 functional regulators shall issue regulations re-

1 garding the policies, procedures, and controls
2 required by paragraph (1) applicable to the fi-
3 nancial institutions that are subject to their re-
4 spective enforcement authority under section
5 523.

6 “(B) SPECIFIC REQUIREMENTS.—The reg-
7 ulations required by subparagraph (A) shall—

8 “(i) require the chief compliance offi-
9 cer or chief executive officer of a financial
10 institution to personally attest that the
11 customer information security system of
12 the financial institution is in compliance
13 with Federal and other applicable stand-
14 ards and is subject to an ongoing system
15 of monitoring;

16 “(ii) require audits by the issuing
17 agency (or submitted to the issuing agency
18 by an independent auditor paid for by the
19 financial institution to audit the financial
20 institution on behalf of the issuing agency)
21 of the customer information security sys-
22 tem of a financial institution not less fre-
23 quently than once every 5 years;

24 “(iii) require the imposition by the
25 issuing agency of appropriate monetary

1 penalties for failure to comply with appli-
2 cable customer information security stand-
3 ards; and

4 “(iv) include such other requirements
5 or restrictions as the issuing agency con-
6 siders appropriate to carry out this section.

7 “(C) EFFECTIVE DATE.—Regulations
8 issued under this paragraph shall become effec-
9 tive 6 months after the effective date of the Fi-
10 nancial Privacy Protection Act of 2005.

11 “(b) NOTIFICATION TO CUSTOMERS OF UNAUTHOR-
12 IZED ACCESS TO CUSTOMER INFORMATION.—

13 “(1) FINANCIAL INSTITUTION REQUIREMENT.—

14 In any case in which there has been a breach at a
15 financial institution, or such a breach is reasonably
16 believed to have occurred, the financial institution
17 shall promptly notify—

18 “(A) each customer whose customer infor-
19 mation was or is reasonably believed to have
20 been accessed in connection with the breach or
21 suspected breach;

22 “(B) the appropriate Federal functional
23 regulator or regulators with respect to the fi-
24 nancial institutions that are subject to their re-
25 spective enforcement authority;

1 “(C) each consumer reporting agency de-
2 scribed in section 603(p) of the Fair Credit Re-
3 porting Act; and

4 “(D) appropriate law enforcement agen-
5 cies, in any case in which the financial institu-
6 tion has reason to believe that the breach or
7 suspected breach affects a large number of cus-
8 tomers, including as described in paragraph
9 (5)(A)(iii), subject to regulations of the Federal
10 Trade Commission.

11 “(2) OTHER ENTITIES.—For purposes of para-
12 graph (1), any person that maintains customer in-
13 formation for or on behalf of a financial institution
14 shall promptly notify the financial institution of any
15 case in which such customer information has been,
16 or is reasonably believed to have been, breached.

17 “(3) TIMELINESS OF NOTIFICATION.—Notifica-
18 tion required by this subsection shall be made—

19 “(A) promptly and without unreasonable
20 delay, upon discovery of the breach or suspected
21 breach; and

22 “(B) consistent with—

23 “(i) the legitimate needs of law en-
24 forcement, as provided in paragraph (4);
25 and

1 “(ii) any measures necessary to deter-
2 mine the scope of the breach or restore the
3 reasonable integrity of the customer infor-
4 mation security system of the financial in-
5 stitution.

6 “(4) DELAYS FOR LAW ENFORCEMENT PUR-
7 POSES.—Notification required by this subsection
8 may be delayed if a law enforcement agency deter-
9 mines that the notification would seriously impede a
10 criminal investigation, and in any such case, notifi-
11 cation shall be made promptly after the law enforce-
12 ment agency determines that it would not com-
13 promise the investigation.

14 “(5) FORM OF NOTICE.—Notification required
15 by this subsection may be provided—

16 “(A) to a customer—

17 “(i) in writing;

18 “(ii) in electronic form, if the notice
19 provided is consistent with the provisions
20 regarding electronic records and signatures
21 set forth in section 101 of the Electronic
22 Signatures in Global and National Com-
23 merce Act;

24 “(iii) if the number of people affected
25 by the breach exceeds 500,000 or the cost

1 of notification exceeds \$500,000, or a
2 higher number or numbers determined by
3 the Federal Trade Commission, such that
4 the cost of providing notifications relating
5 to a single breach or suspected breach
6 would make other forms of notification
7 prohibitive, or in any case in which the fi-
8 nancial institution certifies in writing to
9 the Federal Trade Commission that it does
10 not have sufficient customer contact infor-
11 mation to comply with other forms of noti-
12 fication with respect to some customers,
13 then for those customers, in the form of—

14 “(I) a conspicuous posting on the
15 Internet website of the financial insti-
16 tution, if the financial institution
17 maintains such a website; and

18 “(II) notification through major
19 media in all major cities and regions
20 in which the customers whose cus-
21 tomer information is suspected to
22 have been breached reside, that a
23 breach has occurred, or is suspected,
24 that compromises the security, con-
25 fidentiality, or integrity of customer

1 information of the financial institu-
2 tion; or

3 “(iv) in such additional forms as the
4 Federal Trade Commission may by rule
5 prescribe; and

6 “(B) to consumer reporting agencies and
7 law enforcement agencies (where appropriate),
8 in such form as the Federal Trade Commission
9 shall by rule prescribe.

10 “(6) CONTENT OF NOTIFICATION.—Each notifi-
11 cation to a customer under this subsection shall in-
12 clude—

13 “(A) a statement that—

14 “(i) credit reporting agencies have
15 been notified of the relevant breach or sus-
16 pected breach; and

17 “(ii) notwithstanding any other provi-
18 sion of law, the customer may elect to
19 place a fraud alert in the file of the con-
20 sumer to make creditors aware of the
21 breach or suspected breach, and to inform
22 creditors that the express authorization of
23 the customer is required for any new
24 issuance or extension of credit (in accord-

1 ance with section 605A of the Fair Credit
2 Reporting Act); and

3 “(B) such other information as the Federal
4 Trade Commission determines is appropriate.

5 “(7) COMPLIANCE.—Notwithstanding para-
6 graph (5), a financial institution shall be deemed to
7 be in compliance with this subsection, if—

8 “(A) the financial institution has estab-
9 lished a comprehensive customer information
10 security system that is consistent with the
11 standards prescribed by the appropriate Federal
12 functional regulator under subsection (a);

13 “(B) the financial institution notifies af-
14 fected customers and consumer reporting agen-
15 cies in accordance with its own internal infor-
16 mation security policies in the event of a breach
17 or suspected breach; and

18 “(C) such internal security policies incor-
19 porate notification procedures that are con-
20 sistent with the requirements of this subsection
21 and the rules of the Federal Trade Commission
22 under this subsection.

23 “(8) RULES OF CONSTRUCTION.—

24 “(A) IN GENERAL.—Compliance with this
25 subsection by a financial institution shall not be

1 construed to be a violation of any provision of
2 subtitle A, or any other provision of Federal or
3 State law prohibiting the disclosure of financial
4 information to third parties.

5 “(B) LIMITATION.—Except as specifically
6 provided in this subsection, nothing in this sub-
7 section requires or authorizes a financial insti-
8 tution to disclose information that it is other-
9 wise prohibited from disclosing under subtitle A
10 or any other applicable provision of Federal or
11 State law.

12 “(c) CIVIL PENALTIES.—

13 “(1) DAMAGES.—Any customer adversely af-
14 fected by an act or practice that violates this section
15 may institute a civil action to recover damages aris-
16 ing from that violation.

17 “(2) INJUNCTIONS.—Actions of a financial in-
18 stitution in violation or potential violation of this
19 section may be enjoined.

20 “(3) CUMULATIVE EFFECT.—The rights and
21 remedies available under this section are in addition
22 to any other rights and remedies available under any
23 other provision of applicable State or Federal law.

24 “(d) CIVIL ACTIONS BY STATE ATTORNEYS GEN-
25 ERAL.—

1 “(1) AUTHORITY OF STATE ATTORNEYS GEN-
2 ERAL.—In any case in which the attorney general of
3 a State has reason to believe that an interest of the
4 residents of that State has been or is threatened or
5 adversely affected by an act or practice that violates
6 this section, the State may bring a civil action on be-
7 half of the residents of that State in a district court
8 of the United States of appropriate jurisdiction, or
9 any other court of competent jurisdiction—

10 “(A) to enjoin that act or practice;

11 “(B) to enforce compliance with this sec-
12 tion;

13 “(C) to obtain—

14 “(i) damages in the sum of actual
15 damages, restitution, or other compensa-
16 tion on behalf of affected residents of the
17 State; and

18 “(ii) punitive damages, if the violation
19 is willful or intentional; or

20 “(D) obtain such other legal and equitable
21 relief as the court may consider to be appro-
22 priate.

23 “(2) RULE OF CONSTRUCTION.—For purposes
24 of bringing any civil action under paragraph (1),
25 nothing in this section shall be construed to prevent

1 an attorney general of a State from exercising the
2 powers conferred on the attorney general by the laws
3 of that State—

4 “(A) to conduct investigations;

5 “(B) to administer oaths and affirmations;

6 or

7 “(C) to compel the attendance of witnesses
8 or the production of documentary and other evi-
9 dence.

10 “(3) VENUE.—Any action brought under this
11 subsection may be brought in the district court of
12 the United States that meets applicable require-
13 ments relating to venue under section 1931 of title
14 28, United States Code.

15 “(4) SERVICE OF PROCESS.—In an action
16 brought under this subsection, process may be
17 served in any district in which the defendant—

18 “(A) is an inhabitant; or

19 “(B) may be found.”.

20 **SEC. 3. DEFINITIONS.**

21 Section 527 of the Gramm-Leach-Bliley Act (15
22 U.S.C. 6827) is amended—

23 (1) by redesignating paragraph (4) as para-
24 graph (6);

1 (2) by redesignating paragraphs (1) through
2 (3) as paragraphs (2) through (4), respectively;

3 (3) by inserting before paragraph (2), as rededesignated,
4 the following:

5 “(1) BREACH.—The term ‘breach’—

6 “(A) means the unauthorized acquisition,
7 disclosure, or loss of computerized data or
8 paper records which compromises the security,
9 confidentiality, or integrity of customer information,
10 including activities proscribed under
11 section 521; and

12 “(B) does not include a good faith acquisition
13 of customer information by an employee or
14 agent of a financial institution for a business
15 purpose of the institution, if the customer information
16 is not subject to further unauthorized
17 disclosure.”;

18 (4) in paragraph (2), as redesignated—

19 (A) by striking “person) to whom” and inserting
20 the following: “person)—

21 “(A) to whom”; and

22 (B) by striking the period at the end and
23 inserting the following: “; and

24 “(B) with respect to whom the financial institution
25 maintains information in any form, re-

1 gardless of whether the financial institution is
2 providing a product or service to or on behalf
3 of that person.”;

4 (5) in paragraph (3), as redesignated—

5 (A) by striking “institution’ means any”
6 and inserting the following: “institution’—

7 “(A) means any”;

8 (B) by inserting “(regardless of whether
9 the financial institution is providing any prod-
10 uct or service to or on behalf of that customer)”
11 before “and is identified”; and

12 (C) by striking the period at the end and
13 inserting the following: “; and

14 “(B) for purposes of section 522, includes
15 the last name of an individual in combination
16 with any 1 or more of the following data ele-
17 ments, when either the name or the data ele-
18 ments are not encrypted:

19 “(i) Social security number.

20 “(ii) Driver’s license number or State
21 identification number.

22 “(iii) Account number, credit or debit
23 card number, or any required security
24 code, access code, or password that would

1 permit access to a financial account of the
2 individual.

3 “(iv) Such other information as the
4 Federal functional regulators determine is
5 appropriate with respect to the financial
6 institutions that are subject to their re-
7 spective enforcement authority.”; and

8 (6) by inserting before paragraph (6), as redes-
9 igned, the following:

10 “(5) FEDERAL FUNCTIONAL REGULATOR.—The
11 term ‘Federal functional regulator’ has the same
12 meaning as in section 509, and includes the Federal
13 Trade Commission.”.

14 **SEC. 4. INCLUSION OF FRAUD ALERTS IN CONSUMER**
15 **CREDIT REPORTS.**

16 Section 605A of the Fair Credit Reporting Act (15
17 U.S.C. 1681c-1) is amended—

18 (1) in subsection (b)(1), by inserting “or proof
19 of a notification of a breach or suspected breach
20 under section 522(b)(1)(C) of the Gramm-Leach-Bliley Act” after “theft report”; and

22 (2) by adding at the end the following:

23 “(i) NO ADVERSE ACTION BASED SOLELY ON FRAUD
24 ALERT.—It shall be a violation of this title for the user
25 of a consumer report to take any adverse action with re-

1 spect to a consumer based solely on the inclusion of a
2 fraud alert, extended alert, or active duty alert in the file
3 of that consumer, as required by this subsection.”.

4 **SEC. 5. STUDIES AND REPORTS ON IMPROVING PROTEC-**
5 **TION OF CUSTOMER INFORMATION.**

6 (a) ALTERNATIVE INFORMATION STORAGE METH-
7 ODS.—

8 (1) STUDY.—The Federal Trade Commission
9 shall conduct a study of alternative technologies, in-
10 cluding biometrics, that may be used by financial in-
11 stitutions and other businesses to enhance the safe-
12 guarding of the customer information of financial in-
13 stitutions and other sensitive personal information.
14 Such study shall include an analysis of how to en-
15 sure that such information does not become wide-
16 spread or subject to theft.

17 (2) REPORT TO CONGRESS.—The Commission
18 shall submit a report to the Congress on the results
19 of the study conducted under paragraph (1) not
20 later than 6 months after the date of enactment of
21 this Act.

22 (b) TRANSPORTATION OF CUSTOMER INFORMA-
23 TION.—

24 (1) STUDY.—The Comptroller General of the
25 United States, in consultation with the Federal func-

1 tional regulators and appropriate law enforcement
2 agencies, shall conduct a study of the cross country
3 transport of the customer information of financial
4 institutions and other sensitive personal information
5 by or on behalf of financial institutions and other
6 businesses.

7 (2) REPORT TO CONGRESS.—The Comptroller
8 General shall submit a report to the Congress on the
9 results of the study conducted under paragraph (1)
10 not later than 6 months after the date of enactment
11 of this Act, including any recommendations on ways
12 that financial institutions may best reduce the risk
13 of compromise, breach, or loss of the customer infor-
14 mation of financial institutions and other sensitive
15 personal information during transport.

16 **SEC. 6. EFFECTIVE DATE.**

17 This Act and the amendments made by this Act shall
18 take effect 6 months after the date of enactment of this
19 Act.